PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-161172
(43)Date of publication of application : 23.06.1995

(51)Int.Cl. G11B 23/28
G11B 23/30

(21)Application number : 05-304214
(22)Date of filing : 03.12.1993

(71)Applicant : SONY CORP
(72)Inventor : IMURA SHIGERU

(54) DATA RECORDING MEDIUM

(57)Abstract:
PURPOSE: To record various data with high security in a manner to be convenient to use to a recording medium such as a disca tape or the like.
CONSTITUTION: A recording medium 12 where data are recorded is accommodated in a case 11. An IC 20 is installed at a predetermined position of the case 11. A start program and ciphered data are recorded in the recording medium 12and a cipher program of the recorded data and data of password Nos. are stored in a memory in the IC 20. When the recorded data are to be read out or when data are to be written in the recording medium 12.an input password No. is sent to the 1C 20 and compared with the password No. stored in the memory in the IC 20 by an operational means. When tone password Nos. agree with each otherciphered data recorded in the recording medium 12 are decoded or data to be recorded to the recording medium 12 are ciphered according to the cipher program stored in the memory in the IC 20.

CLAIMS

[Claim(s)]
[Claim 1]In a data recording medium which makes a predetermined case store a recording medium on which data is recorded by a predetermined methodand attaches to a prescribed spot of this case IC which has a memory and a calculating meansData enciphered by the above-mentioned recording medium as a boot program is made to recordA memory in the above-mentioned IC is made to memorize a data encryption program enciphered [above-mentioned] and data of

a passwordWhen reading data recorded on the above-mentioned recording mediumor when writing data in the above-mentioned recording mediumWhen you make the above-mentioned IC supply an inputted passworda password and a calculating means which were memorized by memory in this IC make it compare and a password is in agreementA data recording medium which could be made to perform encryption of data recorded on enciphered decoding or the above-mentioned recording medium of data which was recorded on the above-mentioned recording medium according to an enciphered program memorized by memory in IC.
[Claim 2]The data recording medium according to claim 1 which was made to perform a block to which an enciphered program is not made to output by collation of a password within IC when [at which it set beforehand] prescribed time continuation is carried out and disagreement is detected even if a password is in agreement by future collation.
[Claim 3]The data recording medium according to claim 2 been made to cancel a block by making a password set up apart from the above-mentioned password in the state defined beforehand where carried out prescribed time continuationdetected disagreementand it was blocked input.
[Claim 4]The data recording medium according to claim 1 it was made to make a memory in IC memorize additional information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]This invention relates to the data recording medium applied to various recording mediasuch as magnetic diskssuch as a floppy diska magneto-optical discan optical discand magnetic tape.
[0002]
[Description of the Prior Art]As a recording medium which records a computer program etc.the magnetic disk called a floppy disk etc. is used widely. The magneto-optical disc and optical disc which use a laser beam for record or playback are also used as a medium whose storage density is higher than a magnetic disk.
[0003]In making a program record on these disksFor examplewhen recording data on the sector set as the data recording tracks of each disk and playing into it in an order according to the recording format of this diskit is made to play record data in order of the sector according to a recording formatand he is trying to acquire the recorded program.
[0004]On the other handin order to improve the security nature of the data recorded on the disknot making data record in order of the sector according to

the usual formatbut adding suitable offset etc. to a sector and recording them is performed. Thusif it is not prepared for the computer side which the offset data etc. which made the sector change read when reading the data recorded on the diska right program cannot be acquired but the unauthorized use of a program can be prevented.
[0005]
[Problem(s) to be Solved by the Invention]Howevereven when an order of a sector is made to change in this wayit is possible to reproduce all the data recorded on one disk with the copy device reproduced on another disk as it is. Thereforeif the offset data of the sector required for exact read-out of dataetc. are prepared for the computer side which performs reproduction from an original disk with such a copy deviceand uses the reproduced diskit is possible to reproduce and use a program improperly. Thereforesuch a record method is an imperfect record method from a viewpoint of the prevention from an unauthorized use of a program.
[0006]There is also the method ofenciphering the program data itself to record on the other hand based on a predetermined cipher systemand recording the enciphered data on a disk. In this casethe enciphered program which decodes this program data is requiredManagement of the disk etc. with which this enciphered program was recorded [the necessity of preparing independently the disk etc. with which the enciphered program was recorded] for ** is troublesomeand when this disk is lostdecoding of program data will become impossible. In order to make it decoding according to such loss not become impossibleit is possible to copy the disk with which the enciphered program was recordedbut if an enciphered program is copiedsecurity nature will become low so much and the enciphered meaning will be lost.
[0007]When enciphering in this waythere is also a method of hanging scramble using a certain keywordbut. In such a caseif it is necessary to know the same keyword by the side decrypted [that is enciphered and] and the same keyword is used repeatedlya keyword will become known widely and the meaning of encryption will be lost. Thereforemanagement of a keyword will become complicated although there is also a method of changing the keyword which is called a disposable key word mode and to be used one by one.
[0008]Although the explanation so far explained the case where computer program data was made to record on a diskalso when making data record on other recording mediasuch as magnetic tapethere is same problem about security nature.
[0009]There is the purpose of this invention in the ability to be made to perform user-friendly record whose security nature is highwhen making various datasuch as a programrecord on recording mediasuch as a disk and a tape.
[0010]

[Means for Solving the Problem]In a data recording medium which makes the predetermined case 11 store the recording medium 12 on which data is recorded by a predetermined methodand attaches to a prescribed spot of this case 11 IC20 which has a memory and a calculating means as this invention is shownfor example in drawing 1Data enciphered by the recording medium 12 as a boot program is made to recordA memory in IC20 is made to memorize an enciphered data encryption program and data of a passwordWhen reading data recorded on the recording medium 12or when writing data in the recording medium 12When you make an inputted password supply to IC20a password and a calculating means which were memorized by memory in this IC20 make it compare and a password is in agreementAccording to an enciphered program memorized by memory in IC20it can be made to perform encryption of data recorded on enciphered decoding or the recording medium 12 of data which was recorded on the recording medium 12.
[0011]In this casewhen [at which it set beforehand] prescribed time continuation is carried out and disagreement is detectedeven if a password is in agreement by future collationit is made to perform a block to which an enciphered program is not made to output by collation of a password within IC.
[0012]It is made to cancel a block by making a password set up apart from the above-mentioned password in this state where it was blocked input.
[0013]When it mentions aboveit is made to make a memory in IC memorize additional information.
[0014]
[Function]According to this inventionthe enciphered program of the data recorded on the recording mediumThe security nature which decoding of the data which was memorized by IC attached to the case which stores this recording mediumcould not read an enciphered program from this IC unless the password was in agreementtherefore was recorded on the recording medium cannot be performedeitherand prevents the unauthorized use of the recorded data is high.
[0015]In this caseby collation of the password within ICwhen [at which it set beforehand] prescribed time continuation is carried out and disagreement is detectedeven if a password is in agreement by future collationthe effect of preventing unjust use by performing the block to which an enciphered program is not made outputting becomes higher.
[0016]By making the password set up apart from the password for enciphered program read-out in this state where it was blocked inputit is having been made to cancel the block and release in the state where it was blocked can be performed good.
[0017]IC the enciphered program was remembered to be is efficiently used for the memory in IC by making additional information memorize.
[0018]
[Example]Hereafterworking example of this invention is described with

reference to an accompanying drawing.
[0019]In this exampleit is what was applied to the data recording medium for computers which uses the magnetic disk called a floppy diskand as shown in drawing 1 - drawing 3it constitutes. Drawing 1 is a figure showing the entire configuration of the floppy disk of this exampleten in a figure shows the whole floppy diskinto the case 11 in which this floppy disk 10 was formed with the synthetic resinthe magnetic disk 12 3.5 inches in diameter is storedand the shutter 13 which can be opened and closed freely is attached. The window part 13a is formed in this shutter 13when the shutter 13 is an opened statethe position of the opening 11a by the side of the case 11 and the window part 13a is in agreementand the signal recording surface of the magnetic disk 12 is exposed.
[0020]And when the drive which mentions this floppy disk 10 later is made to equipthe magnetic disk 12 rotates by a predetermined driving meansand a magnetic head approaches the signal recording surface which the shutter 13 was in the opened state and exposedand record and playback of data can be performed with this head. This signal recording surface may have been formed in the case of only one sideand both sides. So farit is the composition of the usual floppy disk.
[0021]And IC(integrated circuit) 20 of one chip makes it build in the corner of the case 11 of this floppy disk 10 in this example. It has supposed that it is this IC20 that the eight points of contact 2122and 23 and ....28 were only exposed as expanded and shown in drawing 2 if it sees from the surface of the case 11and the internal circuit is embedded in the resin which constitutes the case 11 in drawing 3 as a section shows. The composition inside IC20 is mentioned later.
[0022]Nextthe composition of the drive of the floppy disk 10 constituted in this way is explained. Drawing 4 and drawing 5 are the figures showing the composition of this driveand 30 in a figure is shownand the whole floppy disk driving this floppy disk driving 30It is connected the motor 32 side by the predetermined chucking mechanism 33and the floppy disk 10 which has the window part 31 for equipping with the floppy disk 10 and with which the inside was equipped from this window part 31 is rotated to a prescribed speed by the motor 32as a section shows to drawing 5. And record and playback are performed by the magnetic head which is not illustratedthe record data supplied from the host computer side mentioned later is recorded on the magnetic disk 12and the data played from the magnetic disk 12 is supplied to the host computer side.
[0023]And in order to connect with the eight points of contact 21-28 exposed to the surface of the floppy disk 10the terminal unit 40 is formed and it is made to have contacted the points of contact 21-28 to which eight the contact pieces 4142and 43 and the tips of ....48 which were allotted to this terminal

unit 40 correspondedrespectively. And each contact pieces 41-48 are connected to the predetermined interface by the side of a host computerand it is control by the side of a host computerand can be made to perform processing of read-out of stored data etc.
[0024]Nextif the composition of IC20 built in the floppy disk 10 of this example is explainedas shown in drawing 6Six [21-26] of the eight points of contact 21-28 are used hereThe point of contact 21 is used as the power supply terminal VCCand it is considered as the program-voltages input terminal VPP of EEPROM55 in which the point of contact 22 was built inThe point of contact 23 is made into serial-data input/output terminal I/Othe point of contact 24 is used as the clock input terminal CLKthe point of contact 25 is used as the reset signal input terminal RSTand the point of contact 26 is set to earthing terminal GND.
[0025]And the prime controller (CPU) 51 which performs data processing as a circuit inside IC20The serial/parallel-conversion circuit 52 for performing a data input/output between the exteriors in IC20The counting-down circuit 53 for supplying the clock for conversion to this serial/parallel conversion 52RAM54 which memorizes data temporarilyand EEPROM55 which memorize data preservation and rewriting[of a password etc.] It comprises ROM56 which memorizes programssuch as an enciphered programand is connected by the bus line between the prime controller 51the serial/parallel-conversion circuit 52and each memories 5455and 56.
[0026]And to the prime controller 51 and the counting-down circuit 53the clock obtained by the point of contact 24 (clock input terminal CLK) is suppliedand the prime controller 51 operates to them based on this clock. In this casethe prime controller 51 is started by the point of contact 25 (reset pulse input terminal RST) by a predetermined reset signal being supplied. The signal which carried out dividing of the clock with the counting-down circuit 53 is supplied to the serial/parallel-conversion circuit 52and conversion to parallel data from serial data or conversion to serial data from parallel data is performed based on this dividing signal. And the point of contact 23 (serial-data input/output terminal I/O) as an input/output terminal with the exterior is connectedthe serial data supplied via the point of contact 23 are changed into parallel data from the exteriorand the serial/parallel-conversion circuit 52 is supplied via a bus line at the prime controller 51 etc. The parallel data supplied to the serial/parallel-conversion circuit 52 via a bus line are changed into serial dataand are supplied to the external computer (host computer) side from the point of contact 23.
[0027]The data memorized by EEPROM55 of this IC20 is that predetermined program voltages are supplied to the point of contact 22 (program-voltages input terminal VPP) from the exteriorand rewriting of it is enabled.

[0028]Nextthe composition by the side of the floppy disk 10 by which this IC20 was built inand the host computer accessed is explained. Drawing 7 is a figure showing the composition of this host computerand 61 in a figure is shownand the main prime controllers (CPU) to this prime controller 61. The floppy disk interface 62the hard disk unit 63RAM64ROM65the keyboard interface 66the CRT interface 68and the serial/parallel-conversion circuit 69 are connected via the bus line. And the floppy disk interface 62The interface by the side of the record data by the side of the magnetic disk 12 of the floppy disk 10 with which the floppy disk driving 30 mentioned above was equippedand the prime controller 61 is performedand. The interface IC20 built in the floppy disk 10 and by the side of the prime controller 61 is performed.
[0029]The keyboard 67 makes it have connected with the keyboard interface 66and the operation information on the keyboard 67 is transmitted to the prime controller 61 side via the interface 66. CRT display device 70 is connectedthe indicative data supplied via a bus line is supplied to the CRT display device 70 sideand the corresponding character and picture are displayed on the CRT interface 68. It enables it to have transmitted data to the external instrument (peripheral equipmentsuch as a printer: not shown) connected via the serial/parallel-conversion circuit 69.
[0030]And between the host computer constituted in this way and IC20 in the floppy disk 10communication is performed by processing as shown in drawing 9and data processing which uses IC20 is performed. That isthe signal of predetermined potential is first supplied as the power supply VCC and the program voltages VPP from the host computer sideand the clock CLK of predetermined frequency is supplied and the state where IC20 can operate is set up (Step 201). The reset signal of a low level "L" is supplied in the state of this beginningand it changes into the state where the prime controller 51 in IC20 was reset.
[0031]And the reset pulse RST is changed to high level"H"reset is canceledand IC20 is started (Step 202). Herewhen IC20 startsan initial data required for data exchange as a reply signal is transmitted to the host computer side from the prime controller 51 in IC20 (Step 203). The information etc. which determine a logical levela first bitetc. of the data which IC20 receives are included in this initial data.
[0032]And in the prime controller 61 side of a host computerif this initial data is receivedthe interface of IC20 will be set as the state where it correspondedand future sessions will be performed. Nexta command is made to transmit to the prime controller 51 in IC20 from a host computer (Step 204). This command comprises 5 bytesfor exampleand shows the attribute of command structurea commanda parameteretc.
[0033]And in the prime controller 51 of IC20the transmitted command belongs to

the command structure given to this ICIand the authentication data which moreover judges whether a command and a parameter are the rightand is carried out as a result of judging is returned to a host computer (Step 205). When the authentication data judged that a command is normal is returnedthe data corresponding to a command is made to transmit continuously (Step 206). This direction of a data transfer is set up by a command. There may be no data transfer depending on a command.

[0034]And the status which finally shows that the processing by the side of IC20 was completed is transmitted to the host computer side (Step 207)and this session is ended. Thena host computer repeats from the command transmission of Step 204 to status reception of Step 207 if needed.

[0035]And the command of two systems is prepared as a command used in this case in this example. That isit is a command treated without preparing a management command as the 1st command and being known by the userand is the command by which use was permitted only to the publisher and administrator of the floppy disk 10.

[0036]And access at the time of the 2nd command using the floppy disk 10 by the command which controls the interface of IC20 using this command is performed.

[0037]Although the floppy disk 10 with a built-in IC of this example is used with the composition explained abovean example of processing in the case of using followingamong these ICharbored 20 is explained with reference to the flow chart of drawing 8.

[0038]The program data for computers is made to encipher and record on the magnetic disk 12 in the floppy disk 10and ROM56 in IC20 is made to memorize the enciphered program here. The boot program required to read the recorded program data is made to record on the magnetic disk 12. This boot program is not made to encipher. And it enables it to set the password (number in the number of a predetermined beam) for reading an enciphered program from IC20 as IC20and the data of this set-up password is made to save EEPROM55 in IC20. Apart from the password for this enciphered program read-outthe password for block release mentioned later is also set upand it is made to save EEPROM55 in IC20.

[0039]And only when the same number as the password registered into EEPROM55 is supplied from the host computer sideit enables it to have read the enciphered program memorized in IC20 to the host computer side. It has been made to perform block processing which the registered password is control of the prime controller 51 in IC20 when the input process of this mistaken password is performed succeeding the case where a different number is inputted3 timesand forbids read-out of the enciphered program from this IC20. In this state where it was blockedeven if a right password is inputtedread-out

of an enciphered program is forbidden.
[0040]And the block is canceled when the same number as the password for block release registered into EEPROM55 is supplied from the host computer side in this state where it was blocked. Howeverwhen the input of the password for this block release is mistaken continuously 10 timesas the prime controller 51 in IC20 does not receive the input of the password for block release itselfit has been made to be carried out in the higher-level block. Unless the administrator (floppy disk issue-origin) of this SEKYU rete system cancels using the tool for managementit is made to have not returned to the state where it can access with IC20where this high-level block is performed.
[0041]It enables it to have memorized the additional information (arbitrary informationincluding an easy table of contentsa datea user nameetc.) about the program which was enciphered by the magnetic disk 12 and recorded on it which does not need to be enciphered in the memories (RAM54 etc.) in IC20.
[0042]The processing in the case of playing the data which was enciphered in this way and recorded on the magnetic disk 12 in the floppy disk 10 (or enciphering to the magnetic disk 12 data record) is explained in order according to the flow chart of drawing 8 below. Firsta host computer reads the boot program recorded on the magnetic disk 12and is made to read it in a host computer (Step 101). This operation is the same as the operation at the time of starting of the program currently recorded on the conventional floppy disk.
[0043]And it is made to indicate that CRT display device 70 by the side of a host computer has an input request of a password after this startup (Step 102). When alter operation of a password is performed by the keyboard 67this inputted data of a number is made to transmit to IC20 in the floppy disk 10 after this display (Step 103). And if the status from IC20 is received by the host computer side (Step 104)it will be judged whether IC20 is blocked with the data received at this time (Step 105).
[0044]When blocked at this timeit is made to indicate blocked by CRT display device 70 by the side of a host computer (Step 106). When the authentication result of whether a password is in agreement when not blocked is judged (Step 107) and a code case is in agreementa mode input is performed by operation of the keyboard 67 etc. (Step 109). This mode input is for choosing whether the additional information memorized by IC20 is read or read-out of an enciphered program is performed.
[0045]When a password is not in agreement at Step 107after giving an indication which requires reinput of a password to CRT display device 70 by the side of a host computer (Step 109)it returns to Step 103.
[0046]And after a mode input is performed at Step 109it is judged whether it is that the mode in which the prime controller 61 by the side of a host computer was inputted is what checks additional information (Step 110). Herein

not being the mode in which additional information is checkedit performs processing which makes the enciphered program memorized by ROM56 in IC20 transmit to RAM64 by the side of a host computer (Step 111). And judge whether it is that the processing needed at this time is the processing (processing made to write in) which data is made to record on a floppy disk (Step 112)and in making it record. It is considered as the data which had data to record encipheredand this enciphered data is made to record on the predetermined sector of the magnetic disk 12 by the processing by the side of the host computer based on the enciphered program transmitted to RAM64 (Step 113). The additional information (data of a recording date etc.) produced at this time is made to transmit to IC20and the area which memorizes additional information is made to memorize (Step 114).

[0047]And when it judges that it is the processing (processing made to read) reproduced at Step 112. By the processing by the side of the host computer based on the enciphered program which played the predetermined data recorded on the magnetic disk 12made transmit to the host computer sideand was transmitted to RAM64. Decrypt the played datathe drive (hard disk or other floppy disks) side which had this decrypted data specified is made to supplyand it is made to write in (Step 115).

[0048]And after processing of this record and reproduction is completedthe purging process which makes the enciphered program which RAM64 by the side of a host computer has memorized eliminate is performed (Step 116). After the erasing processing of this enciphered program is completedit judges whether the session of IC20 required at this time was completed (Step 117)and when it endsit returns to the processing which uses DOS (disc operating system) by the side of a host computer (Step 118).

[0049]In being the mode in which additional information is checked at Step 110the additional information memorized by IC20 is made to read into the host computer side (Step 119)and it displays this read additional information on CRT display device 70 (Step 120). And if this display is performedit will move to Step 117.

[0050]And when it judges that the session of IC20 is not completed at Step 117it returns to Step 108 and is made to perform again from mode input processing.

[0051]After indicating blocked at Step 106When it judges whether the alter operation of the password for block release occurs by the keyboard 67 (Step 121) and this alter operation occursthis inputted data of the password for block release is made to transmit to IC20 (Step 122). And if the status from IC20 is received by the host computer side (Step 123)authenticating processing of whether the password for block release was in agreement will be performedand it will be judged whether it was in agreement (Step 124).

Herewhen in agreementit moves to Step 108 and a mode input is received. When not in agreementaccess with IC20 is ended and it returns to the processing which moved to Step 118 and uses DOS by the side of a host computer.
[0052]The unauthorized use of the data enciphered and recorded by using the floppy disk 10 as mentioned aboveand record and playback of the enciphered data being performed can be prevented effectively. That iswhen IC20 built in the floppy disk 10 memorizes and it performs record and playback on a diskand only when the password is knownthe program about the method of enciphering reads this enciphered programand has come to be able to perform a data encryption and decryption. For this reasonunless a password is knowncan decode the recorded datacannot read it and the preventive effect of an unauthorized use is highand it is difficult to read and copy an enciphered programand there are few possibilities that an enciphered program will leak outside.
[0053]Thereforeeven if it reproduces the data recordedfor example on one floppy disk using the device copied altogether as it isthe enciphered program itself is not reproduced but the program data recorded on the floppy disk is prevented from being used improperly.
[0054]Since the boot program required to read the recorded program data in this example was recorded on the magnetic disk 12without encipheringOperation until it reads this boot program by the control from a host computerIf it is the same as the conventional floppy disk and the processing which reads an enciphered program according to this boot program is made to be performedIt is not necessary to prepare a control program special for encryption or decryptionand can realize at the host computer side by control of the same program configuration as the case where the conventional floppy disk is used.
[0055]Since the disk and the enciphered program correspond by 1 to 1 when IC20 is made to build in one floppy disk like this examplean enciphered program is changeable for every one floppy disk. By thusthe thing for which an enciphered program is changed for every one floppy disk. Even if which enciphered program of a metaphor leaks outsideall the record data of the disk with which this system is applied cannot be decoded only by only the data of the specific disk corresponding to this enciphered program being decipherableand an unauthorized use preventive effect becomes higher.
[0056]When in this example multiple-times (above-mentioned working example 3 times) continuation is carried out and collation processing of a password is performed accidentallySince read-out of the enciphered program from built-in IC was blocked noting that a possibility of trying to read an enciphered program unjustly was highIt keeps the work which those who do not know a password perform collating work repeatedlyand decodes a password from being possibleand the preventive effect of the unauthorized use also from this point is high.

[0057]Among thesewhere read-out of the enciphered program from harbored IC is blockedSince it is made to be made of another password to cancel this block statusCan perform management when blocked easily and the collating work of the password for canceling this block statusSince read-out of the enciphered program from built-in IC was thoroughly blocked when multiple-times (above-mentioned working example 10 times) continuation was carried out and it carried out accidentallythe effect over prevention of an unauthorized use is still higher.
[0058]In above-mentioned working examplewhen record and playback to a floppy disk were performedmake an enciphered program transmit to the host computer side from IC20and were made to perform processing of encryption or decryption within the host computerbut. As read-out of the enciphered program from IC20 cannot be performedit may be made to encipher the data recorded on decryption and the disk of the data instead played from the disk by the processing in IC20. In this casesince an enciphered program is not transmitted outside at allthere is no possibility that an enciphered program will be copied by the host computer sideand security nature is dramatically high. Howevercompared with the case where it is necessary to make the data played from the diskand the data recorded on a disk once transmit to IC20and to make it processand it is processed by the host computer sideplayback and record of data take time a little.
[0059]Although above-mentioned working example did not explain an encryption method in particularvarious encryption methods applicable to the data for computers can be used. For examplethe method of enciphering for every number of bytes equivalent to one sector of a floppy diskthe method of enciphering for every number of bytes equivalent to one trackthe method of bundling up data and a program and encipheringetc. can be considered. When enciphering for every predetermined sector or trackit may be made to change an encryption algorithm for every unit data of this to encipher. It may be made to encipher only some data of the data recorded on one floppy disk.
[0060]Although it was made to make IC20 memorize the additional information of the data recorded on a disk in above-mentioned working exampleit enciphers as occasion demands and may be made to make it memorize also about this additional information. It may be made to make it record on the predetermined area of the magnetic disk 12 instead of making IC20 memorize.
[0061]Although it applied to the magnetic disk in above-mentioned working exampleof courseit is applicable to other recording media. For exampleit is applicable also to the recording medium of the shape of a disksuch as a magneto-optical disc and an optical discand the recording medium of the tape shape of magnetic tape etc. In any caseit can be coped with if IC is made to build in the case which stores a recording medium. Various data other than the

program for computers is applicable also to the data recorded on a recording medium.
[0062]
[Effect of the Invention]According to this inventionthe enciphered program of the data recorded on the recording mediumThe security nature which decoding of the data which was memorized by IC attached to the case which stores this recording mediumcould not read an enciphered program from this IC unless the password was in agreementtherefore was recorded on the recording medium cannot be performedeitherand prevents the unauthorized use of the recorded data is high. For exampleit is difficult not to copy the enciphered program which is copied while it had been encipheredand decodes the copied databut to decode the copied dataeven if the user who does not know a password copies the data recorded on the recording medium to another recording mediumand an unauthorized use is prevented.
[0063]In this caseby collation of the password within ICwhen [at which it set beforehand] prescribed time continuation is carried out and disagreement is detectedeven if a password is in agreement by future collationthe effect of preventing unjust use by performing the block to which an enciphered program is not made outputting becomes higher.
[0064]By making the password set up apart from the password for enciphered program read-out in this state where it was blocked inputit is having been made to cancel the block and release in the state where it was blocked can be performed good.
[0065]IC the enciphered program was remembered to be is efficiently used for the memory in IC by making additional information memorize.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a perspective view showing one working example of this invention.
[Drawing 2]It is a top view showing the important section of one working example.
[Drawing 3]It is a sectional view which meets III-III line of drawing 2.
[Drawing 4]It is a top view showing the composition of the disk driving with which the disk of one working example is applied.
[Drawing 5]It is a sectional view which meets the V-V line of drawing 4.
[Drawing 6]It is a lineblock diagram showing built-in IC of one working example.
[Drawing 7]It is a lineblock diagram showing an example of the host computer

connected with built-in IC of one working example.
[Drawing 8]It is a flow chart figure showing the disk writing of one working exampleand read-out processing.
[Drawing 9]It is an explanatory view showing the communicating state of built-in IC of one working exampleand a host computer.
[Description of Notations]
10 Floppy disk
11 Case
12 Magnetic disk
13 Shutter
20 Built-in IC
21222324252627and 28 Point of contact
30 Floppy disk driving
40 Terminal unit
41424344454647and 48 Contact piece
51 Prime controller (CPU)
56 ROM